

A NOTE ON BINARY COMPLETELY REGULAR CODES WITH LARGE MINIMUM DISTANCE

NEIL I. GILLESPIE

ABSTRACT. We classify all binary error correcting completely regular codes of length n with minimum distance $\delta > n/2$.

1. INTRODUCTION

We consider codes of length n as subsets of the vertex set $V(\Gamma) = \mathbb{F}_2^n$ of the binary Hamming graph Γ , which is endowed with the *Hamming metric* $d(-, -)$. The graph Γ has automorphism group $\text{Aut}(\Gamma) = \mathfrak{B} \rtimes \mathfrak{L}$, where $\mathfrak{B} \cong S_2^n$ and $\mathfrak{L} \cong S_n$ [2, Thm. 9.2.1], and because \mathfrak{B} acts regularly on \mathbb{F}_2^n , we may identify \mathfrak{B} with the group of translations of \mathbb{F}_2^n and \mathfrak{L} with the group of permutation matrices in $\text{GL}(n, 2)$. We say two codes of length n are *equivalent* if there exists $x \in \text{Aut}(\Gamma)$ that maps one to the other. For a code C in Γ , the *minimum distance*, δ , of C is the smallest distance between distinct codewords. For $\alpha \in \mathbb{F}_2^n$, the *distance of α from C* is $d(\alpha, C) = \min\{d(\alpha, \beta) : \beta \in C\}$, and the *covering radius*, ρ , of C is the furthest distance any vertex in \mathbb{F}_2^n is from C . We let C_i denote the set of vertices in \mathbb{F}_2^n that are *distance i from C* . (For all unexplained concepts, see [2, Sec. 11.1].) We say C is *completely regular* if for $\nu \in C_i$, with $i \in \{0, \dots, \rho\}$, the number $\ell_{ik} = |\Gamma_k(\nu) \cap C|$ depends only on i and k , and not on the choice of ν (here $\Gamma_k(\nu)$ denotes the set of vertices at distance k from ν).

In his paper on completely regular codes, Neumaier [9] posed the problem of classifying various families of completely regular codes. With respect to this question, we classify all binary completely regular codes of length n with $\delta > \max\{2, n/2\}$. An obvious example of one of these codes is the *binary repetition code*, which consists of the all zero and all one vertices. Up to equivalence, there exists only one other.

Theorem 1.1. *Let C be a binary completely regular code with $|C| > 1$ and $\delta > \max\{2, n/2\}$. Then either $\delta = n$ and C is equivalent to the binary repetition code; or $(n, \delta) = (7, 4)$ and C is equivalent \mathcal{H}_E , the even half of the Hamming code given in Example 2.1.*

Remark 1.2. Originally the author believed that Theorem 1.1 could easily be deduced from the classification of binary non-antipodal completely regular codes given by Borges et al. [1]. However, recently Borges communicated to the author that there is a mistake in their classification, specifically stemming

Date: draft typeset October 25, 2012

2000 Mathematics Subject Classification: 94B05, 94C30.

Key words and phrases: completely regular codes, Hamming codes, equidistant codes. This research was supported by the Australian Research Council Federation Fellowship FF0776186 of Winthrop Professor Cheryl Praeger.

from Lemma 14 in their paper. Furthermore, subsequently Rifá and Zinoviev [10] constructed an infinite family of examples that does not appear in their classification with Borges (see the codes of length $n = \binom{m}{2}$ for m even given in [10, Thm. 1(1)]). This led the author to prove Theorem 1.1, and in particular, give a proof that is independent of [1]. Furthermore, this result plays an essential role in the classification of another family of completely regular codes [6].

2. EXAMPLE AND PROOF

For $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_2^n$, the *support* of α is the set $\text{supp}(\alpha) = \{i : \alpha_i \neq 0\}$, and the *weight* of α is $\text{wt}(\alpha) = |\text{supp}(\alpha)|$. We denote the unique vertex with $\text{wt}(\alpha) = 0$, n by $\mathbf{0}$, $\mathbf{1}$ respectively. We say a code C of length n with minimum distance δ is a *linear* $[n, k, \delta]$ -code if it is a k -dimensional subspace of \mathbb{F}_2^n , and in this case, the *external distance* of C is equal to the the number of non-zero weights of the *dual code* of C (see [2, Sec 11.1]). We call a set D of vertices of constant weight k in \mathbb{F}_2^n a t -design if $\mathcal{D} = (N, \mathcal{B})$, where $N = \{1, \dots, n\}$ and $\mathcal{B} = \{\text{supp}(\beta) : \beta \in D\}$, forms a $t - (n, k, \lambda)$ design for some positive integer λ . If C is a binary completely regular code with minimum distance δ that contains $\mathbf{0}$, then it is known that the set $C(k)$ of codewords of weight k , with $\delta \leq k \leq m$, forms a t -design for $t = \lfloor \frac{\delta}{2} \rfloor$, assuming that $C(k) \neq \emptyset$ [7]. We now give a non-trivial example of a binary completely regular code with $\delta > n/2$.

Example 2.1. Let \mathcal{H} be the $[7, 4, 3]$ -Hamming code with the following parity check matrix:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Let \mathcal{H}_E be the even half of \mathcal{H} , so \mathcal{H}_E consists of $\mathbf{0}$ and the set $\mathcal{H}(4)$ of 7 codewords of weight 4. Interestingly, in this case, \mathcal{H}_E is the dual code of \mathcal{H} , and is an equidistant code with minimum distance $\delta = 4$ [8, Sec. 3.3]. Thus, as \mathcal{H} has weight distribution $(1, 0, 0, 7, 7, 0, 0, 1)$, \mathcal{H}_E has external distance $s = 3$. Consequently, because $\delta = 2s - 2$ and \mathcal{H}_E consists of codewords of even weight, it follows that \mathcal{H}_E is completely regular [2, p.347]. Moreover, we deduce that $\mathcal{H}(4)$, which is equal to the set of codewords of weight 4 in \mathcal{H}_E , forms a $2 - (7, 4, 2)$ design.

For a code C with covering radius ρ , the *distance partition* of C is the set $\{C, C_1, \dots, C_\rho\}$, which forms a partition of \mathbb{F}_2^n . The distance partition of a code C is *equitable* if, for all $i \geq 0$, every vertex $x \in C_i$ has the same number c_i of neighbours in C_{i-1} and the same number b_i of neighbours in C_{i+1} . Neumaier [9] proved that a code in the Hamming graph (more generally in a distance regular graph) is completely regular if and only if its distance partition is equitable. In this case, $i(C) = \{b_0, \dots, b_{\rho-1}, c_1, \dots, c_\rho\}$ is the *intersection array* of C . (By definition, $b_\rho = c_0 = 0$.) The following result can be found in [1, Thm 11], but we give a new proof here.

Lemma 2.2. *Let C be a binary completely regular code with $\delta \geq 3$ such that $\mathbf{0} \in C$ and $\mathbf{1} \notin C$. Then C has covering radius $\rho \geq \delta - 1$ and $C_\rho = \mathbf{1} + C$.*

Proof. As $\mathbf{1} \notin C$, it follows that $\mathbf{1} \in C_i$ for some $i \geq 1$. Since C is completely regular, we deduce that $\Gamma_n(\nu) \cap C \neq \emptyset$ for all $\nu \in C_i$. Hence $\mathbf{1} + C_i \subseteq C$. Similarly, because the Hamming graph is a distance regular graph, we deduce from [9, Thm 3.2] that $\Gamma_n(\alpha) \cap C_i \neq \emptyset$ for all $\alpha \in C$, and so $\mathbf{1} + C_i = C$, or equivalently $C_i = \mathbf{1} + C$. Furthermore, for any $j \in \{0, \dots, \rho\}$, it follows that $d(x, C_i) = |i - j|$ for all $x \in C_j$. Thus, if $i < \rho$ then C_i has covering radius $\rho' = \max\{\rho - i, i\} < \rho$, contradicting the fact that C_i is equivalent to C . Hence $i = \rho$. Now let $\{b_0, \dots, b_{\rho-1}, c_1, \dots, c_\rho\}$ be the intersection array of C . If $e = \lfloor \delta - 1/2 \rfloor$, then $c_i = i$ for $i \leq e$ and $b_i = n - i$ for $i \leq e - 1$, and if δ is even then $b_e = n - e$. By [9], C_ρ is completely regular with reverse intersection array. However, because C_ρ is equivalent to C , their intersection arrays are in fact equal. Thus $b_i = c_{\rho-i}$ for $0 \leq i \leq \rho - 1$. Now suppose that $\rho < \delta - 1$, and so $\rho - e \leq e$. If $\rho - e < e$ then $n - \rho + e = b_{\rho-e} = c_e = e$, and so $n = \rho < \delta - 1$, which is a contradiction. Thus $\rho = 2e$, which implies that $\delta = 2e + 2$. However, in this case $n - e = b_e = c_e = e$, and so $n = \rho < \delta - 1$, again a contradiction. \square

To prove Theorem 1.1, we let C be a binary completely regular code with $|C| > 1$ and $\delta > \max\{2, n/2\}$. By replacing C with an equivalent code if necessary, we can assume that $\mathbf{0} \in C$. If $\delta = n$, it is straight forward to deduce that $C = \{\mathbf{0}, \mathbf{1}\}$. Thus we assume that $\delta < n$. Because C is completely regular, it follows that the set $C(\delta)$ of codewords of weight δ is non-empty. Let $\beta \in C(\delta)$. If $\mathbf{1} \in C$, then $d(\mathbf{1}, \beta) = n - \text{wt}(\beta) < n/2$, contradicting the minimum distance of C . Thus $\mathbf{1} \notin C$. Hence, by Lemma 2.2, C has covering radius $\rho \geq \delta - 1$ and $C_\rho = \mathbf{1} + C$. Consequently, for $\gamma \in C \setminus \{\mathbf{0}\}$, it holds that

$$\frac{n}{2} < \delta \leq \text{wt}(\gamma) \leq n - \rho \leq n - \delta + 1 < \frac{n}{2} + 1.$$

In particular, this implies that n is odd, $\delta = (n + 1)/2$ and $C = \{\mathbf{0}\} \cup C(\delta)$. Furthermore, because C is completely regular, it follows that C is equidistant. Thus, for all $\alpha, \beta \in C(\delta)$, it holds that $d(\alpha, \beta) = \delta$. This implies that δ is even and that $|\text{supp}(\alpha) \cap \text{supp}(\beta)| = (n + 1)/4$ for all $\alpha, \beta \in C(\delta)$. Consequently there exist positive integers e, λ such that $C(\delta)$ forms an $(e + 1) - (n, \delta, \lambda)$ design with $\delta = 2e + 2$ [7]. As $\delta \geq 4$, it follows that $e + 1 \geq 2$. Now, a non-negative integer ℓ is a *block intersection number* of a t -design if there exist two blocks of the design that intersect in exactly ℓ points. We have just shown that the design $C(\delta)$ has only one block intersection number, which is equal to $(n + 1)/4$. If $e + 1 \geq 3$, then $C(\delta)$ is at least a 3-design, and it is known that the only 3-designs with one block intersection number are the ‘degenerate’ cases where $n \in \{\delta, \delta + 1\}$ [4], which in this case cannot hold as $4 \leq \delta < n/2 + 1$. Thus $e + 1 = 2$. This implies that $\delta = 4$ and $m = 7$. Furthermore, because $C(\delta)$ has only one block intersection number, it is a symmetric $2 - (7, 4, \lambda)$ design with $\lambda = (n + 1)/4 = 2$ [3, Thm 1.15]. Recall from Example 2.1 the $[7, 4, 3]$ -Hamming code \mathcal{H} , and the code $\mathcal{H}_E = \mathbf{0} \cup \mathcal{H}(4)$. We saw in Example 2.1 that $\mathcal{H}(4)$ forms a $2 - (7, 4, 2)$ design. The complementary design of this design is a $2 - (7, 3, 1)$ design, which is unique up to isomorphism [5, Table 1.28], and so $\mathcal{H}(4)$ is also unique up to isomorphism. Hence there exists $\sigma \in \mathfrak{L}$ such that $C(\delta)^\sigma = \mathcal{H}(4)$, and because $\mathbf{0}^\sigma = \mathbf{0}$, it follows that $C^\sigma = \mathcal{H}_E$, proving Theorem 1.1.

REFERENCES

- [1] J. Borges, J. Rifà, and V. A. Zinoviev. On non-antipodal binary completely regular codes. *Discrete Math.*, 308(16):3508–3525, 2008.
- [2] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1989.
- [3] P. J. Cameron and J. H. van Lint. *Designs, graphs, codes and their links*, volume 22 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.
- [4] P. J. Cameron. Near-regularity conditions for designs. *Geometriae Dedicata*, 2:213–223, 1973.
- [5] C. J. Colbourn and J. H. Dinitz, editors. *The CRC handbook of combinatorial designs*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.
- [6] N. I. Gillespie and C. E. Praeger. Classification of a family of completely transitive codes. arXiv:1208.0393, 2012.
- [7] J.-M. Goethals and H. C. A. van Tilborg. Uniformly packed codes. *Philips Res. Rep.*, 30:9–36, 1975.
- [8] S. M. Moser and Po-Ning Chen. *A student's guide to coding and information theory*. Cambridge University Press, Cambridge, 2012.
- [9] A. Neumaier. Completely regular codes. *Discrete Math.*, 106/107:353–360, 1992. A collection of contributions in honour of Jack van Lint.
- [10] J. Rifà and V. A. Zinoviev. On a class of binary linear completely transitive codes with arbitrary covering radius. *Discrete Math.*, 309(16):5011–5016, 2009.

[GILLESPIE] CENTRE FOR THE MATHEMATICS OF SYMMETRY AND COMPUTATION, SCHOOL OF MATHEMATICS AND STATISTICS, THE UNIVERSITY OF WESTERN AUSTRALIA, 35 STIRLING HIGHWAY, CRAWLEY, WESTERN AUSTRALIA 6009

E-mail address: neil.gillespie@uwa.edu.au